Os *cybercrimes* e o *cyberbullying* - apontamentos jurídicos ao direito da intimidade e da privacidade

Adriano Roberto Vancim [1]
José Eduardo Junqueira Gonçalves [2]

Sumário: 1 Introdução. 2 Hackers e crackers. 3 Os vírus e a internet. 3.1 Outras artimanhas. 4 Da criminalidade virtual. 5 O ciberbullying. 6 Intimidade e privacidade na web. 6.1 Posição jurisprudencial. 7 Considerações finais. 8 Referências bibliográficas.

1 Introdução

Como cediço, inegável em tempos atuais a corrente prática delitiva por meio da internet, às vezes até como um novo meio instrumental de operacionalização do crime, às vezes o surgimento de uma nova modalidade de tipificação delitiva, o que recomenda maior estudo e aprofundamento desta eclosão criminosa que certamente não parará por aí.

A este respeito, incisivas são as práticas delitivas prescritas pelos *hackers* ou outros criminosos virtuais, que vez por outra se utilizam de diversas artimanhas de informática a perpetrar infrações aos direitos da personalidade, direito à intimidade e privacidade, e mesmo até ao direito de propriedade, sendo inúmeros os casos de fraude jurídica promovida pela internet ora capituladas como furto mediante fraude, ora como estelionato, a depender da real intenção deliberada e consciente na aferição da vantagem ilícita e do *modus operandi*.

Como se não bastasse, também hoje cristalina a prática do *bullying* virtual, ou *cyberbullying*, que, em grande parte das vezes, se reveste de ato infracional passível de repreensão pelo Código Penal brasileiro ou mesmo, a depender da legitimidade, pelo Estatuto da Criança e do Adolescente - ECA, o que não descaracteriza sua inserção penal como *cybercrime*.

Por uma ou outra via jurídica, fato é que o Direito não pode se distanciar da finalidade primacial de pacificação e resolução da lide, muito menos encontrar impedimento a tanto, devendo ser utilizada, por ora, nossa legislação vigente, a coibir a crescente prática dessas infrações criminosas.

Por óbvio, entrementes, ante a assombrosa e reconhecida evolução tecnológica, outras modalidades de crime certamente permearão nossa esfera jurídica, dentre as quais as hipóteses de "pichação eletrônica", "difusão de vírus" e "a pescaria e o estelionato com uso de redes", em distinta e precisa observância ao que explicita o eminente Desembargador Fernando Neto Botelho (2011):

> Essa engenharia do mal, que monopoliza o conhecimento (da computação sofisticada e dos protocolos de redes), cresce à sombra da impunidade gerada pela insuficiência regulamentar de desatualizados instrumentos legais do país, como o Código Penal de 2010. Para cuidar da nova realidade, só lei atualizada. A tecnologia, sozinha, não dará conta. Só a lei garante oportunidade de defesa e prova justa, próprias das Democracias amadurecidas.

Nesse escopo, sem que se tenha a pretensão de esgotar o assunto, extremamente complexo, apenas pautamos em contribuir com e auxiliar em maior discussão do assunto em tela, tão usualmente corrente em nossa seara jurídica, pedindo vênia, como modo de maior compreensão, ao expor alguns tópicos de ordem técnico-informática.

2 *Hackers* e *crackers*

Talvez reconhecidos como os grandes vilões criminosos na internet, sem poder afastar a figura de outras "tribos delitivas", tem-se que o primeiro uso da expressão de *hackear* no mundo da informática foi de alguém que conhecia de modo muito detalhado um sistema operacional a ponto de poder obter desse sistema o que desejasse. Assim, um *hacker* seria simplesmente alguém que tivesse conhecimento detalhado desses sistemas operacionais e assim o utilizasse a seu livre talante, por óbvio sem autorização e às vezes sem conhecimento de seu legítimo detentor.

A grande verdade é que os *hackers* são muito bons e sabem escrever códigos que realmente funcionam. São pessoas que detêm um conhecimento acima da média, em níveis informáticos. São seres que conhecem quais são as falhas de um sistema operacional ou mecanismos (frutos do conhecimento e da informação) que permitem a invasão de plataformas alheias.

Já os *crackers*, cujo termo foi cunhado em 1985 pelos próprios *hackers*, com o inequívoco objetivo de não serem confundidos, são aqueles que rompem a segurança de um sistema em busca de informações confidenciais com o objetivo de causar danos ou obter vantagens pessoais. Pode-se assegurar que, ao contrário dos *hackers*, os *crackers* manifestam, preponderantemente, intenções criminosas, em suas diversas espécies e modalidades.

---

[1] Advogado licenciado. Servidor público vinculado ao Juizado Especial Cível e Criminal e Vara da Infância e Juventude da Comarca de Guaxupé/MG. Professor colaborador, conteudista da disciplina Direito Administrativo no curso de Pós-Graduação da Faculdade de Educação São Luís/SP. Autor de vários artigos jurídicos. Autor e coautor de obras jurídicas.

[2] Juiz de Direito do Estado de Minas Gerais. Diretor do Foro e Titular da Unidade Jurisdicional do JESP da Comarca de Guaxupé e Juiz da Vara da Infância e Juventude da Comarca de Guaxupé/MG. Membro da Academia Ourofinense de Letras e Artes. Ex-parecerista e Assessor Jurídico da Câmara Municipal de Ouro Fino/MG. Coautor da obra Ramalhete - Poesias reunidas. Ex-professor de ensino fundamental e médio com formação em Teologia pelo Instituto de Formação Cristã.

Exemplificativamente, a descoberta de uma falha em determinado *browser* (que deixa o internauta desprotegido quando velejando pela rede) pode ser feita por alguém interessado em solucionar a questão de segurança, por mero repto intelectual, como, outrossim, pode ser feita por alguém com objetivos escusos, fraudatórios, de espionagem ou meramente vandálicos.

Conclusivamente, em termos distintos, o *hacker* é aquele que é atiçado exclusivamente pelo desafio intelectual de romper as defesas de um sistema operacional - e aí encerrar sua batalha mental, sem, contudo, deliberada intenção delitiva. Já o *cracker* pode ser diferenciado no sentido de que é ele quem inicia sua batalha quando do rompimento das defesas do sistema operacional sob ataque, tendo em vista a obtenção de benefícios para si ou para outrem, sempre em detrimento de terceiros, em nítida finalidade delitiva.

Muitas vezes, para conseguir seu objetivo, utilizam-se de programas especializados criados pelos próprios, conhecidos popularmente como "vírus", conforme veremos a seguir.

3 Os vírus e a internet

Vírus são simplesmente programas. Todos eles. No tipo mais comum de vírus eles são programas muitos pequenos e invisíveis. O computador (ou melhor dizendo, o sistema operacional), por si só, não tem como detectar a existência deste programa. Ele não é referenciado em nenhuma parte dos seus arquivos, ninguém sabe dele, e ele não costuma se mostrar antes do ataque fatal.

Os vírus nada têm a ver, diretamente, com a internet. São programas que se instalam no seu computador quando você executa um programa já infectado, causando danos, e já existiam bem antes dela. Mas o crescimento da internet certamente contribuiu em muito para a disseminação dos vírus, pois facilitou enormemente a troca de arquivos entre computadores, o que antes era feito basicamente por meio de disquetes. Do mesmo modo que os vírus se propagam por meio de arquivos contaminados em disquetes, também o fazem através de arquivos transmitidos via internet.

Um dos tipos mais utilizados para invasão de sistemas operacionais é o "cavalo de tróia". O nome se deve a uma analogia ao poema clássico escrito por Homero - *Ilíada*, no qual os gregos, após anos de lutas infrutíferas com o intuito de transpassar as muralhas da antiga cidade de Tróia, ardilosamente se esconderam em um cavalo feito de madeira e com ele presentearam os troianos, conseguindo dessa forma invadir os domínios da cidade sem serem percebidos.

Atualmente, o vírus com essa denominação, funcionando da forma como narrado acima, é um tipo de programa que, uma vez instalado em seu computador, proporciona uma maneira de alguém entrar sem ser percebido, muito conhecido também pelo nome em inglês, *trojan horse*.

3.1 Outras "artimanhas"

Além das citadas modalidades em que o sistema operacional dos computadores são "atacados" por nefastos programas, podemos citar ainda, a título de exemplo corriqueiro, os *spamming*, *spam*, *cookies*, *spywares, hoaxes, sniffers, phishing* e *keilogger*.

Os *spamming* correspondem ao envio não consentido tampouco querido ou desejado pelo receptor de incessantes e inúmeras mensagens publicitárias por correio eletrônico a um número muitíssimo elevado de usuários da rede.

O *spam* consiste na prática de criar malas diretas com endereços eletrônicos copiados de forma escusa a fim de "bombardear" as caixas postais alheias com mensagens indesejadas.

Além dessa peleja jurídica com relação ao *spam*, onde o objeto é sua ilicitude, comumente, este método de *web marketing* é muito utilizado para propiciar invasões de sistemas operacionais, da mesma forma que os "cavalos de tróia" supracitados.

A seu modo, os *cookies* são pequenos arquivos de textos que são gravados no computador de determinado usuário, assim hospedados quando da visita a outros sites de comércio eletrônico. Assim, o usuário passa a ter o controle de forma a identificar o computador com um número específico e único, permitindo o acesso e obtenção de informações quanto ao reconhecimento de quem está acessando o *site*, de onde decorre e com que periodicidade com que é visitado, dentre outras informações que desejar.

Já o objetivo dos *spywares* é o envio de informações do computador do usuário da rede a outras pessoas desconhecidas, como programas espiões que são, seja por meio do acesso do servidor assim que o usuário está *on-line*, seja pelo envio de informações via *e-mail*.

Os *hoaxes* são *e-mails* que possuem conteúdos alarmantes e falsos, em boa parte das vezes apontando como remetentes empresas importantes no cenário nacional ou internacional, ou mesmo órgãos governamentais de reconhecida atuação administrativa e empresarial, às vezes até levando à prática de crime contra a economia popular (como as "correntes" e "pirâmides"), podendo, ainda, estar acompanhados por vírus.

Por sua vez, os *sniffers*, também reconhecidos como programas espiões, visam basicamente rastrear e reconhecer o conteúdo e a leitura dos *e-mails* que circulam na rede mundial de computadores, em nítida e convicta afronta aos primados básicos à digressão normativa.

Os *phishing* podem ser definidos ou mesmo evidenciados como a emissão de *e-mails* enganosos, que induzem os destinatários a abrir um arquivo, contaminando o computador.

Já os *keilogger* são programas que registram praticamente tudo o que é teclado e que aparece na tela do computador, geralmente com a finalidade de auferir senhas, mas podem, todavia, ser tolhidos pelo uso e instalação de anti-*spywares* e *firewalls*.

Assim, reconhecem-se sem pormenores diversas fraudes cometidas mediante manipulação de computadores, em boa parte com a manipulação de dados de "entrada" (subtração de dados), mediante a manipulação de programas, seja pelo aspecto modificativo ou até pela deturpação dos programas, com manipulação de dados de "saída" ou pela manipulação técnico-informática.

Pode-se aduzir também a incessante prática de falsificações informáticas nas modalidades de falsificação do objeto (ao alterar dados de documentos rigidamente armazenados) ou falsificação do instrumento (hipótese em que o computador serve para efetuar falsificações de documentos, em geral, de uso comercial).

Não se pode olvidar, ainda, os correntes danos e modificações de programas ou dados do computador, fenômeno tratado como "sabotagem informática", caso em que, sem nenhuma autorização a respeito, documentos ou programas são modificados em sua originalidade, às vezes pela introdução de vírus, pelo acesso não autorizado a sistemas de serviços e, substancialmente, pela reprodução não consentida e autorizada de programas informáticos de proteção.

4 Da criminalidade virtual

Na década de 1960 apareceram os primeiros casos de crimes informáticos na imprensa e literatura científica. Foi divulgada pela primeira vez a utilização do computador para a prática de delitos, constituídos por manipulações, sabotagens, espionagem e uso exacerbado de computadores e sistemas. Após uma década do surgimento, iniciaram-se os estudos sistemáticos e científicos, com emprego de métodos criminológicos, estudando-se um número restrito de delitos informáticos denunciados, entre os quais alguns de grandes reflexos na Europa, por envolverem empresas mundialmente famigeradas.

Já em 1980 houve crescimento de ações criminosas incidentes em manipulações de caixas bancárias, pirataria de programas de computador e abusos nas telecomunicações, deixando transparecer vulnerabilidades que os criadores do processo não previram. Acresce-se aqui o delito de pornografia infantil na rede, comumente disseminado na época.

Essa criminalidade, no entender de Luiz Flávio Gomes (2003, p. 68-9):

> conta com as mesmas características da informatização global: transnacionalidade - todos os países fazem uso da informatização (qualquer que seja o seu desenvolvimento econômico, social ou cultural); logo, a delinquência correspondente, ainda que em graus distintos, também está presente em todos os continentes; universalidade - integrantes de vários níveis sociais e econômicos já têm acesso aos produtos informatizados (que estão se popularizando cada vez mais); ubiquidade - a informatização está presente em todos os setores (públicos e privados) e em todos os lugares.

Dentro desse contexto, reconhece-se, como fator criminógeno, que a informática é permissiva quanto ao cometimento de novos delitos e potencializa outros tradicionais, exemplificando, o estelionato. Sendo assim, os crimes podem ser cometidos com o computador - *the computer as a tool of a crime* - e cometidos contra o computador (informações e programas nele contidos) - *the computer as the object of a crime*.

A conceituação de crimes digitais fornecida pelo autor Gustavo Testa Corrêa (2003, p. 69) é de "todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar". Ao analisar essa definição, detecta-se que há menção aos crimes cometidos contra o computador, mas não só contra as informações e programas nele contidos, como também contra as informações e dados em trânsito por computadores, com o dolo de ameaça e fraude, não atingindo os crimes realizados com o computador, contudo, cujo bem tutelado pelo ordenamento jurídico é diverso, como ocorre com a pedofilia.

Em uma segunda corrente, Reginaldo César Pinheiro (2001, p. 18-9) classifica os crimes informáticos ou cibernéticos em três categorias: virtuais puros, mistos ou comuns.

> O crime virtual puro seria toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, o equipamento e seus componentes, inclusive dados sistemas. Crime virtual misto seria aquele em que o uso da internet é condição *sine qua non* para a efetivação da conduta, embora o bem jurídico visado seja diverso do informático, como, por exemplo, as transferências ilícitas de valores em uma *homebanking* ou no chamado *salamislacing*, onde o *cracker* retira de milhares de contas correntes, diariamente, pequenas quantias que correspondem a centavos e as transfere para uma única conta. Embora esses valores sejam ínfimos para o correntista, que, na maioria das vezes, nem se dá conta do furto, representam para o cibercriminoso uma expressiva quantia em seu montante. Por derradeiro, crime virtual comum seria utilizar a internet apenas como instrumento para a realização de um delito já tipificado pela lei penal. Assim, a Rede Mundial de Computadores acaba por ser apenas mais um meio para a realização de uma conduta delituosa. Se antes, por exemplo, o crime como o de pornografia infantil (art. 241 do ECA) era instrumentalizado por meio de vídeos ou revistas, atualmente, dá-se por salas de bate-papo, ICQ, como também pela troca de fotos por *e-mail* entre pedófilos e divulgação em *sites*. Mudou a forma, mas a essência do crime permanece a mesma.

Na visão de Ivette Senise Ferreira (2003, p. 69), a definição para crime de informática é "toda ação típica, antijurídica e culpável, cometida contra ou pela

utilização de processamento automático de dados ou sua transmissão". O conceito de ação funda-se em comportamento humano comissivo ou omissivo correspondente ao modelo previsto em lei como crime (típico), com a respectiva penalidade, atentado ao princípio da legalidade que direciona o Direito Penal, acrescendo-se o conceito de crime se a conduta ilícita e a responsabilidade penal puderem ser atribuídas ao agente.

A autora adota a classificação proposta por Hervé Croze e Yves Biscunth (2003, p. 69), na qual os crimes de informática se distinguem em duas categorias:

1) os atos dirigidos contra um sistema de informática, por qualquer motivo, verdadeiro núcleo da criminalidade informática, por se tratar de ações que atentem contra o próprio material informático (suportes lógicos ou dados dos computadores); 2) os atos que atentem contra os valores sociais ou outros bens jurídicos, cometidos através de um sistema de informática, que compreenderia todas as espécies de infrações previstas em lei penal.

Entrementes, cabe ressaltar a preocupação existente acerca da tipificação jurídico-legal em que se inserem os crimes praticados na *web*, bem assim a correspondente imputação delitiva, a ponto de se admitir, por parte da doutrina, que nosso atual modelo penal se encontra desprovido de mecanismo jurídico regulador e sancionador de tais condutas, conforme assinalamos.

A respeito, outra não é a lição de Cecílio da Fonseca Vieira Ramalho Terceiro (2011, p. 01):

> Denota-se que, para a sua caracterização, o crime necessita de: a) uma tipificação expressa como crime por lei; b) conduta (comissiva ou omissiva); c) que, sendo expressa como tal, esteja válida ou apta a surtir efeitos perante todos (*erga omnes*). Diz-se, assim, que é o tipo penal, ou seja, a conduta considerada como atentatória à norma.

Pressupõe e escora tal posicionamento o fato de que se faz necessária a tipificação específica em norma penal da capitulação jurídica correspondente, em observância ao princípio maior da legalidade penal, pelo qual não há crime sem lei anterior que o preveja.

Ainda em contínuo ensinamento, assim pondera o mesmo e renomado autor:

> A teoria da tipicidade visa classificar as condutas humanas em normas penais proibitivas, ou, como preferem alguns doutrinadores, em normas negativas, incriminando todos os fatos que possam estar desviados de uma conduta aceita socialmente. Tudo, tendo como paradigma principal, os critérios de censurabilidade da sociedade, formalizando essas ações na legislação criminal. Para os transgressores dessas normas, impõe-se uma sanção penal, que é geralmente a pena privativa de liberdade (2011, p. 02).

Portanto, mister maior análise, mesmo até como maneira de detida compreensão acerca da tipificação e imputabilidade respectiva, como mandamentos primários e substanciais da norma penal, com a ressalva de que também se mostra necessário, com redobrada permissão, o uso da interpretação adaptativa e teleológica a se atingir o viés objetivo jurídico enquanto do aguardo da resolução definitiva do Projeto de Lei nº 84/99 (Lei de *Cybercrimes*).

5 O ciberbullying

Inegavelmente reconhecido como hipótese de cometimento de violência física, moral e psicológica entre crianças e adolescentes, inicialmente disseminadas apenas no âmbito escolar, o *bullying* praticado pela internet vem espantosamente aumentando a cada dia que passa, sobretudo pela irrestrita facilidade de acesso às ferramentas disponíveis nos modernos meios de comunicação.

Assim, essa reconhecida expressão inglesa é utilizada para qualificar comportamentos agressivos de forma intencional e repetitiva, sem que, todavia, esse nefasto comportamento transgressivo apresente qualquer plausível motivação específica e justificável, muito ao revés, apenas se arrima no fato de se maltratar, intimidar, humilhar ou mesmo amedrontar vítimas, como puro e único "objeto de diversão".

A forma em que traduzida pela internet vem hoje sendo o modo mais usual de ocorrência, já que possibilita que agressões sejam provindas e praticadas anonimamente ou, quando no máximo, que seu praticante se camufle e esconda sua identidade por apelidos, tal como corrente por meio de *messenger*, *e-mail*, *orkut*, *facebook* e outros sítios de relacionamento.

Com o crescimento desenfreado, reflexos jurídicos vão se desencadeando gradativamente, exigindo incisiva resolução pela aplicação da legislação vigente, seja de ordem civil, seja de ordem penal, sem olvidar, nesse desiderato, a aplicação das disposições normativas do Estatuto da Criança e do Adolescente - ECA.

Conforme destacado por Márcio Morena Pinto (2011, p. 01),

> sem pretensos exageros, a rede internet tornou-se um verdadeiro paradigma para a rede de informação, uma forma universal caracterizada pela heterogeneidade e fluidez incessante, o que torna cada vez mais difícil encontrar um sentido global que permita circunscrever toda a fenomenologia do novo a uma suposta dominação. Daí a importância de se estabelecer um ramo jurídico com diretrizes próprias, produzindo-se reflexões jurídicas abrangentes e sistemáticas, tencionando esclarecer as novas práticas geradas com o advento da rede, legitimando-as e conduzindo-as gradativamente a uma possível regulamentação.

A título penal, dependendo por óbvio da intenção do agressor, sua prática pode ser tipificada como hipótese de crime de ameaça, racismo, injúria, calúnia, difamação ou até lesão corporal. Em sede de aplicação do ECA, perfeitamente admissível a aplicação dos crimes descritos nos arts. 240 e 241-A, donde se verifica a busca pela

proteção maior, como bem jurídico tutelado, da liberdade e dignidade da criança ou do adolescente.

Na seara civil, todo e qualquer ato desabonador danoso pode ensejar a aplicação indenizatória, mormente pelo ocasionado abalo moral, como *modus* operacional e educacional a balizar o infortúnio. Registre-se até a posição pela qual em casos que tais a responsabilização sopesaria cunho objetivo, não havendo que se comprovar o dolo como elemento caracterizador da ofensa.

A toda sorte, mister o combate jurídico desta ofensiva prática delitiva, tal como corrente em outros ordenamentos, dentre eles o direito norte-americano e, entre nós, antecipadamente louvado pela Lei Estadual nº 14.651, de 12 de janeiro de 2009, editada pelo Estado de Santa Catarina, que propõe a instituição de um "Programa de Combate ao *Bullying*".

6 Intimidade e privacidade na *web*

A questão acerca do direito à intimidade e privacidade na internet vem sendo amplamente discutida e debatida em tempos atuais, com o fito de proibir e solucionar problemas dele emergidos, que invariavelmente vêm ensejando a aplicação de responsabilização civil como modo de resolução da indisposta ofensa, bem assim, em grande parte das vezes, os crimes na *web* vem a afrontar tais direitos.

Em que pese ter sido inculcada a errônea idéia de que a internet simboliza um meio anônimo, como "anarquismo virtual", por meio do qual as pessoas que nela "navegam" são totalmente desconhecidas e imaginárias, principalmente de impossível identificação, o direito a estar só, o privilégio e a autoconsciência têm sido, frequentemente, objeto de violação por meio de várias artimanhas informáticas, passíveis de verificação.

Stefano Rodotá (2000, p. 120) traz a lume a problemática:

> Tem-se a sensação de que cresce a distância entre o mundo velocíssimo da inovação tecnológica e o mundo lentíssimo da proteção sócio-institucional. Quase a todo momento percebe-se a rápida obsolescência das soluções jurídicas reguladoras de um determinado fenômeno técnico, destinadas de um problema apenas.

Fundado e robustecido na Declaração Universal dos Direitos Humanos, no Pacto Internacional sobre Direitos Civis e Políticos e no Pacto de São José da Costa Rica; nossa Constituição da República dispõe ser inviolável a intimidade e a privacidade, assegurada a quem tenha tais direitos violados, dano material e/ou moral decorrente de sua violação (art. 5º, X).

A concepção de liberdade do ser humano está indiscutivelmente amparada no ordenamento jurídico brasileiro, de forma que toda e qualquer violação ao *status* constitucional da intimidade e privacidade ensejará, de outra parte, consequências àquele que aleatoriamente transgredir o conceito.

Como modo elucidativo, assim leciona Taís Gasparian (2003, p. 37):

> a questão da privacidade, no mundo virtual, adquire então uma dimensão maior: a privacidade na Internet é mais privativa do que no mundo real, e sua violação representa um enorme dano, como se a invasão se operasse no ego da própria pessoa.

Entrementes, cabe assinalar como precisão os aspectos da intimidade e da privacidade do ser humano.

Nesse jaez, cabe o registro de Tércio Sampaio Ferraz (2003, p. 31):

> a intimidade é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum). Não é um conceito absoluto de intimidade, embora se possa dizer que o seu atributo básico é o estar só, não exclui e segredo e a autonomia. Nestes termos, é possível identificá-la: o diário íntimo, o segredo sob juramento, as próprias convicções, as situações indevassáveis de pudor pessoal, o segredo íntimo cuja mínima publicidade constrange.

Já a privacidade, para o mesmo autor:

> trata-se de situações em que a comunicação é inevitável (em termos de relação de alguém com alguém que, entre si, trocam mensagens), das quais, em princípio, são excluídos terceiros. Seu atributo máximo é o segredo, embora inclua também a autonomia e, eventualmente, o estar só com os seus [...]. A vida privada pode envolver, pois, situações de opção pessoal (como a escolha do regime de bens no casamento), mas que, em certos momentos, podem requerer a comunicação a terceiros (na aquisição, por exemplo, de um bem imóvel). Por aí ela difere da intimidade, que não experimenta esta forma de repercussão (2003, p. 31).

Pode-se assim inferir que a intimidade é o que cada indivíduo guarda para si, dentro de si e consigo próprio, sendo seu momento de foro íntimo pessoal; não se confundindo de maneira alguma com a privacidade, já que esta pode ser perfeitamente compartilhada com pessoas conviventes ao redor, seja em qualquer setor de comunidade ou convívio social em que permeado.

Por tal, vem sendo delineado constantemente entendimento quanto ao resguardo desses direitos, como modo de proteger direitos da personalidade humana, inatos por natureza, sendo que condições físicas e morais do ser humano não serão observadas e transparecidas a toda e qualquer pessoa.

Está-se então totalmente imune a ter direito à intimidade e privacidade violados, bem como amplamente protegidos? Seria forçoso, em princípio, referendar tais assertivas de forma absoluta entre o extremo díspare existente entre a evolução tecnológica, e principalmente a internet, e a ciência jurídica Direito, haja vista que, sendo o Direito instrumento regulador de fatos sociais, estes são tutelados no momento oportuno em que vão eclodindo.

Corroborando, límpida é a posição de Danilo César Maganhoto Doneda (2000, p. 118-119), para quem

> a facilidade com que podem e cada vez mais poderão ser obtidas informações pessoais lança, porém, uma sombra sobre a privacidade, capaz de gerar, como potencial conseqüência, a diminuição da esfera de liberdade do ser humano. Numerosos outros fatores agregam-se, o que pode ser exemplificado pelos efeitos da pesquisa atualmente realizada pelo Projeto Genoma, destinado a mapear o código genético e humano e, assim, proporcionar um tratamento que de outra forma seria impossível para diversas patologias. O uso indiscriminado de informações genéticas pessoais, obtidas graças à técnica desenvolvida pelo projeto, por potenciais empregadores, em um único exemplo, pode determinar a exclusão incontinenti desta pessoa do mercado de trabalho e mesmo privá-la de uma vida digna se por acaso possuir predisposição genética para determinada doença.

Objetivando incessantemente prevenir e coibir sempre que situações como a apresentada possam emergir e levar à tona informações personalíssimas ao direito do indivíduo, ocasionando insuportáveis condições indignas e injustas, é que aspectos da intimidade e da privacidade na internet se tornaram uma tônica de remodelamento do aparelho jurídico pátrio.

Pela normatização esculpida pelo Código Civil, foram contemplados e elevados tais direitos à condição de direitos à personalidade, o que significa dizer que estes são imutáveis, irrenunciáveis e inalienáveis.

Não obstante os direitos subjetivos à personalidade terem sido tutelados juridicamente desde a antiguidade, como, por exemplo, em Roma e Grécia, onde se punia com vigor ofensas físicas e morais à pessoa, respectivamente pelos institutos da *actio injuriarum* e *dike kakegorias,* somente após o advento do atual *Codex* Civil é que tais direitos foram reconhecidos e elevados à específica proteção jurídica, como direito subjetivo de cada pessoa em defender o que lhe é próprio, outrora não especificado pelo Código Civil de 1916.

Bem por isso se mostrava a larga preocupação em normatizar tais direitos, sem olvidar, entretanto, que a doutrina e jurisprudência já os mencionavam como "direitos inatos", "inerentes à pessoa humana" ou "primordiais", dos quais não se podia negar sua existência e efeito jurídico deles emergidos, ao ser transcrito no item 17, c, da exposição de motivos do atual Código Civil, que

> todo um novo capítulo foi dedicado aos Direitos da Personalidade, visando à sua salvaguarda, sob múltiplos aspectos, desde a proteção dispensada ao nome e à imagem até o direito de se dispor do próprio corpo para fins científicos ou altruísticos. Tratando-se de matéria de per si complexa e de significação ética essencial, foi preferido o enunciado de poucas normas dotadas de rigor e clareza, cujos objetivos permitirão os naturais desenvolvimentos da doutrina e jurisprudência.

O saudoso mestre R. Limongi França (1975, p. 411) foi quem detalhadamente apresentou inigualável estrutura e classificação a tais direitos, mencionando como direitos da personalidade a defesa à integridade física, intelectual e moral, comportando a proteção à vida humana, aos alimentos, ao próprio corpo, à liberdade de pensamento, à liberdade civil, à honra, à imagem, à identidade pessoal e familiar, dentre vários outros dos quais não cabe aqui analisar, em vista do objetivo perquirido com o presente trabalho.

Pode-se acentuar que os direitos da personalidade possuem como arrimo em nossa Constituição Federal a salvaguarda à dignidade da pessoa humana, de sorte que, nos termos aduzidos pela professora Maria Helena Diniz (2003, p. 119):

> reconhece-se nos direitos da personalidade uma dupla dimensão: a axiológica, pela qual se materializam os valores fundamentais da pessoa, individual ou socialmente considerada, e a objetiva, pela qual consistem em diretos assegurados legal e constitucionalmente, vindo a restringir a atividade dos três poderes, que deverão protegê-los contra quaisquer abusos [...].

Assim é que, nas palavras de Ênio Santarelli Zuliani (2002, p. 45), em citação a Roberto Rosas, outro não é o posicionamento senão em referendar que

> a Constituição Federal deu apoio ao Código Civil como *ius civile*, como uma sobrevida para tutelar o fundamento da dignidade humana (art. 1°, III, da Constituição Federal). E o fez porque o processo constituinte tratou do indivíduo como seu maior fundamento, uma tendência de socialização do Direito.

Destoa, assim, que a tutela dos direitos da personalidade corresponde e eleva cada vez mais o fundamento constitucional da dignidade da pessoa humana, amparados, igualmente, em diversos princípios, hoje tão profundos e acolhidos nesta nova era jurídica denominada "Pós-Positivista", dentre os quais o direito à intimidade e privacidade.

6.1 Posição jurisprudencial

A respeito, em superior instância vêm sendo repelidas tais práticas delitivas e afrontosas, cuja resolução na esfera civil bem acaba por culminar na responsabilização e consequente aplicação de indenização a título de dano moral.

Assim, exemplificativamente:

> Indenização. Dano moral. Ofensas através de site de relacionamento na internet. Responsabilidade civil objetiva. Teoria do risco. Dever de indenizar. Quantum indenizatório. Fixação. - O provedor de serviço de internet, ao disponibilizar espaço em sites de relacionamento virtual, em que seus usuários podem postar qualquer tipo de mensagem, sem prévia fiscalização, e, ainda, com procedência, muitas vezes, desconhecida, assume o risco de gerar danos a outrem, sendo de se aplicar a eles a teoria do risco. O parágrafo único do art. 927 do Código Civil adota a teoria do risco, estabelecendo que

haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar risco para os direitos de outrem. Ao fixar o valor da indenização, devem-se ter em conta as condições do ofendido, do ofensor e do bem jurídico lesado (TJMG, 12ª CC, Apelação Cível n° 1.0091.08.011925-7/001, Rel. Des. Alvimar de Ávila, pub. em 26.04.2010).

Indenização. Dano moral. Orkut. - O prestador do serviço orkut responde de forma objetiva pela criação de página ofensiva à honra e imagem da pessoa, porquanto abrangido pela doutrina do risco criado; decerto que, identificado o autor da obra maligna, contra ele pode se voltar, para reaver o que despendeu (TJMG. Ap. Cível n° 1.0701.08.221685-7/001. Rel. Des. Saldanha da Fonseca, j. em 05.08.2009).

Apelação cível. Indenização por danos morais. Internet. Ofensas veiculadas no orkut. Responsabilidade subjetiva. Ilegitimidade passiva do provedor. - O operador do *site*, em regra, como no caso do orkut, não tem um controle editorial prévio, mas somente *a posteriori*, quando toma conhecimento do que foi efetivamente publicado. Por isso, somente pode ser responsabilizado quando tem conhecimento real do caráter ilícito ou algum motivo para desvendar a natureza da informação. É a partir deste momento, em que é informado do caráter danoso da informação hospedada em seu sistema, que tem a obrigação de tomar todas as medidas necessárias para prevenir danos ou retirá-la, sob pena de ser responsabilizado por negligência. [...]. (TJMG, 9ª Câmara Cível, Apelação Cível n° 1.0024.07.483036-5/001, Rel. Des. Pedro Bernardes, j. em 07.04.2009).

Direito civil. Indenização por danos morais. Texto divulgado na internet. Violação da honra objetiva. Configuração do dano moral à pessoa jurídica. Valor indenizatório. Proporcionalidade e razoabilidade. Recurso parcialmente provido. - Ao escrever e divulgar o *e-mail* narrando fato ocorrido dentro do estabelecimento de dança, a requerida extrapolou os limites de um mero protesto e violou a esfera extrapatrimonial da autora. A pessoa jurídica, portadora de honra objetiva, faz jus à indenização por dano moral sempre que seu nome, credibilidade ou imagem forem abalados por ato ilícito. O magistrado não pode se afastar dos princípios da proporcionalidade e da razoabilidade no momento de fixar o valor da indenização por dano moral, servindo a indenização como instrumento de caráter pedagógico preventivo e educativo da reparação moral (TJDF, 20060110313453APC, Rel. Des. Lécio Resende, 1ª Turma Cível, j. em 14.04.2010, *DJ* de 27.04.2010, p. 88).

Veja-se, pois, que, além da corrente posição acerca da responsabilização de ordem penal, que, frise-se, requer atualizada normatização correspondente, à altura vem sendo aplicado o direito civil como forma de recompor o *status quo ante*, em vista do abalo moral ocasionado pela prática delitiva, cujo modo de operação vem incessantemente se realizando pela internet.

7 Considerações finais

Ante nossa singela exposição, mormente em apenas nos atermos a práticas criminosas ofensivas aos direitos da intimidade e da privacidade, não há como negar sua ascensão na *web*, tal como hodiernamente vem ocorrendo com o *bullying* virtual.

Em que pese a inexistência de legislação penal específica, o Direito vem respondendo com celeridade e mesmo eficiência às demandas criminosas eclodidas, não se podendo olvidar a necessidade de capitulação jurídica de novas hipóteses delitivas que vêm sendo perpetradas pela *web*, o que se espera pela aprovação e publicação do Projeto de Lei n° 84/99.

Corretamente, não se mostra de boa técnica que o indivíduo que se sirva da internet de boa-fé e legitimado a exercer seus direitos essenciais sofra pela incúria que em nada teve correlação delitiva, razão por que afirmativamente vem sinalizando a doutrina e jurisprudência em atribuir ao site-provedor a responsabilização em casos que tais, hoje ainda mais presente nas situações em que há intensa participação dos *hackers* ou dos *crackers*.

Prevalece, pois, a mantença dos direitos da personalidade, em consonância com a intimidade e privacidade, que em nenhuma situação ou circunstância admite seu acoitamento. Pela aplicação do instituto da reparação civil, esculpida pelo Codex Civil e pela Constituição da República, nosso País vem dando um grande salto no que concerne à obstaculização de transgressões lesivas pela internet, destacando-se, a toda evidência, a força imperativa advinda de nosso ordenamento jurídico.

Uma vez mais, apenas cabe frisar que nosso País vem se destacando e se fortalecendo no combate às transgressões criminais expostas e correntes na *web*, muito embora esteja à míngua de uma legislação específica.

8 Referências bibliográficas

BOTELHO, Fernando Neto. Cybercrime. Artigo publicado no Jornal *Valor Econômico* do dia 27.07.2011.

CORRÊA, Gustavo Testa. *Aspectos jurídicos da internet*. São Paulo: Saraiva, 2000, p. 43, apud GUIMARÃES, José Augusto Chaves; FURLANETO NETO, Mário. Crimes na internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*, Brasília, ano VII, n. 20, p. 69, jan./mar. 2003.

DINIZ, Maria Helena. *Curso de direito civil brasileiro*. 20. ed. São Paulo: Saraiva, v.1, 2003.

DONEDA, Danilo César Maganhoto. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo. *Problemas de direito civil constitucional*. Renovar: Rio de Janeiro, 2000.

FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). *Direito e internet*: aspectos jurídicos relevantes. Bauru:

Edipro, 2000, p. 207-237, *apud* GUIMARÃES, José Augusto Chaves; FURLANETO NETO, Mário. Crimes na internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*, Brasília, ano VII, n. 20, p. 69, jan./mar. 2003.

GASPARIAN, Taís. Privacidade em tempos de internet. *Revista do Advogado*, ano XXIII, nº 69, p. 37, maio 2003.

GOMES, Flávio Luiz. *Crimes informáticos*. Disponível em: www.direitocriminal.com.br. Acesso em 26 nov. 2000, *apud* GUIMARÃES, José Augusto Chaves; FURLANETO NETO, Mário. Crimes na internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*, Brasília, ano VII, n. 20, p. 68-69, jan./mar. 2003.

GUIMARÃES, José Augusto Chaves; FURLANETO NETO, Mário. Crimes na internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*, Brasília, ano VII, n. 20, p. 68-69, jan./mar. 2003.

LIMONGI FRANÇA, R. *Manual de direito civil*. 3. ed. Revista dos Tribunais, 1975.

PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. São Paulo: IBCCRIM, v. 101, p. 18-19, abr. 2001 (separata) *apud* GUIMARÃES, José Augusto Chaves; FURLANETO NETO, Mário. Crimes na internet: elementos para uma reflexão sobre a ética informacional. *Revista CEJ*, Brasília, ano VII, n. 20, p. 69, jan./mar. 2003.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. Jus Navigandi, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em: <http://jus.uol.com.br/revista/texto/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais>. Acesso em: 29 jun. 2011.

SOSA, Marcelo Gonçalves. *O bullying na internet*: alguns apontamentos jurídico-sociais. Disponível em file:///F:/Âmbito%20Jurídico%20-%20Leitura%20de%20Artigo%20-%20bulling%20na%20internet.htm . Acesso em 09.08.2011.

ZULIANI, Ênio Santarelli. Reflexões sobre o novo Código Civil. *Revista do Advogado*, nº 68, Ed. AASP, dezembro/2002.

...